关联事件和合规性事件

以下主题介绍如何查看关联事件和合规性事件。

查看关联事件

当活动的关联策略中的关联规则触发时，系统生成关联事件并将其记录至数据库。

注释 当活动的关联策略中的合规 allow 名单触发时，系统生成 an allow 名单事件。

您可以查看关联事件表，然后根据查找的信息操作事件视图。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

您在访问关联事件时看到的页面将随您所使用的工作流程而变化。您可以使用预定义的工作流程，其中包括关联事件的表视图。还可创建自定义工作流程，仅显示匹配特定需求的信息。

开始之前

您必须是 管理员 或 安全分析师 用户才能执行此任务。

过程

步骤 1 选择**分析** > **关联** > **关联事件** 。

或者，要使用不同的工作流程，包括自定义工作流程，请按工作流程标题点击（**切换工作流程**）**([switch workflow])**。

提示 如果使用的是不包含关联事件表视图的自定义工作流程，请点击（**切换工作流程**）**([switch workflow])**，然后选择**关联事件 (Correlation Events)**。

步骤 2 或者，调整时间范围，如更改时间窗口中所述。

步骤 3 执行下列操作之一：

- 要了解有关显示的列的详细信息，请参阅关联事件字段，第 2 页。
- 要查看 IP 地址的主机配置文件，请点击显示在 IP 地址旁边的主机配置文件。
- 要查看用户身份信息，请单击显示在**用户身份 (User Identity)** 旁的用户图标，或对于与 IOC 相关联的用户，请单击**红色用户 (Red User)**。
- 要对事件进行排序和限制，或者要在当前工作流程页面中导航，请参阅使用工作流程。
- 要在当前工作流程中的页面之间导航，保留当前限制，请点击工作流程页面左上角相应的页面链接。
- 要向下展开到工作流程中的下一个页面，限制具体值，请参阅使用向下钻取页面。
- 要删除部分或全部关联事件，请选中要删除的事件旁边的复选框，然后点击**删除 (Delete)** 或点击**全部删除 (Delete All)**，并确认要删除当前限制视图中的所有事件。
- 要导航至其他事件视图以查看关联事件，请参阅工作流程间导航。
- 要查看 Firepower 系统外部可用源中的数据，请右键单击事件值。您看到的选项取决于数据类型，包括公共源；其他来源取决于您配置的资源。有关信息，请参阅使用基于 Web 的资源的事件调查
- 要收集有关事件的情报，请右键单击表中的事件值，然后从思科或第三方情报源中进行选择。例如，您可以从思科 Talos 获取有关可疑 IP 地址的详细信息。您看到的选项将取决于数据类型以及系统上配置的集成。有关详细信息，请参阅使用基于 Web 的资源的事件调查。

相关主题

数据库事件限制
工作流程页面

关联事件字段

当关联规则触发时，系统会生成关联事件。下表介绍关联事件表中可以查看和搜索的字段。

表 *1:* 关联事件字段

字段	说明
说明	关联事件的说明。说明中的信息取决于规则触发方式。 例如，如果操作系统的信息更新事件触发规则，则系统显示新的操作系统名称和可信度。
设备	生成触发策略违规的事件的设备的名称。

字段	说明
域	其受监控流量触发了策略违规的设备的域。 仅当曾经配置Cisco Secure Firewall Management Center以实现多租户时，此字段才存在。
影响	基于入侵数据、发现数据和漏洞信息之间的关联分配给关联事件的影响级别。 搜索此字段时，有效值（不区分大小写）包括 `Impact 0`、`Impact Level 0`、`Impact 1`、`Impact Level 1`、`Impact 2`、`Impact Level 2`、`Impact 3`、`Impact Level 3`、`Impact 4` 和 `Impact Level 4`。请勿使用影响图标颜色或部分字符串（例如，请勿使用 `blue`、`level 1` 或 `0`）。
“入口接口”(Ingress Interface) 或“出口接口”(Egress Interface)	触发策略违规的入侵或连接事件的入口或出口界面。
“入口安全区域”(Ingress Security Zone) 或“出口安全区域”(Egress Security Zone)	触发策略违规的入侵或连接事件的入口或出口安全区域。
内联结果	以下任一项： • 一个黑色向下箭头，表示系统丢弃触发入侵规则的数据包 • 一个灰色向下箭头，表示如果启用**内联时丢弃 (Drop when Inline)** 入侵策略选项，则系统已经丢弃内联中的数据包、交换或路由部署 • 空白，表示触发的入侵规则未设置为“丢弃并生成事件”(Drop and Generate Events) 使用此字段搜索入侵事件触发的策略违规时，请输入： • `dropped`，用来指定是否已经在内联、交换的或路由的部署中丢弃数据包 • `would have dropped`，用于指定当入侵策略设置为在内联、交换的或路由的部署中丢弃数据包时是否已丢弃数据包 请注意，不管规则状态或入侵策略的丢弃行为如何（包括当内联集处于分流模式下），系统都无法在被动部署情况下丢失数据包。
策略	违反的策略的名称。
优先级	关联事件的优先级，由触发的规则或违规的关联策略的优先级确定。搜索此字段时，请输入 `none` 表示无优先级。

字段	说明
规则	触发策略违规的规则的名称。
安全情报类别 (Security Intelligence Category)	代表或包含触发策略违规的事件中的被受阻的 IP 地址的对象的名称。 搜索此字段时，请指定与触发策略违规的关联事件相关联的安全情报类别。安全情报类别可能是安全情报对象的名称、全局阻止列表、自定义安全情报列表或源，或者情报源中的其中一个类别。
“源大洲”(Source Continent) 或“目标大洲”(Destination Continent)	与触发策略违规的事件中的源或目标主机 IP 地址相关联的大洲。
“源国家/地区”(Source Country) 或“目标国家/地区”(Destination Country)	与触发策略违规的事件中的源或目标主机 IP 地址相关的国家/地区。
“源主机重要性”(Source Host Criticality) 或“目标主机重要性”(Destination Host Criticality)	涉及关联事件的源主机或目标主机的用户分配的主机重要性：无 (None)、低 (Low)、中 (Medium) 或高 (High)。 请注意，只有基于发现事件、主机输入事件或连接事件按规则生成的关联事件才包含源主机重要性。
“源 IP”(Source IP) 或“目标 IP”(Destination IP)	触发策略违规的事件中的源主机或目标主机的 IP 地址。
“源端口/ICMP 类型”(Source Port/ICMP Type) 或“目标端口/ICMP 代码”(Destination Port/ICMP Code)	与触发策略违规的事件有关的源流量的源端口或ICMP类型或者目标流量的目标端口或 ICMP 代码。
“源用户”(Source User) 或“目标用户”(Destination User)	登录触发策略违规的事件中的源主机或目标主机的用户的姓名。
时间	生成关联事件的日期和时间。此字段不可搜索。
计数	与每行中所显示的信息匹配的事件数。请注意，**计数 (Count)** 字段仅在应用了创建两个或多个相同行的约束后才显示。此字段不可搜索

相关主题

事件搜索

使用合规 允许 名单工作流程

Cisco Secure Firewall Management Center 提供了一组工作流程，可用于分析为您的网络生成的 allow 名单事件和违规。工作流程与网络映射和控制面板一起构成关于网络资产合规性的关键信息的来源。

系统为 allow 名单事件和违规提供预定义工作流程。也可创建自定义工作流程。在使用合规 allow 名单工作流程时，可以执行许多常见操作。

开始之前

您必须是 管理员、 安全分析师或 发现管理员 用户才能执行此任务。

过程

步骤 1 使用 **分析** > **关联** 菜单访问 an allow 名单工作流程。

步骤 2 您有以下选择：

- “切换工作流程”(Switch Workflow) - 要使用不同的工作流程（包括自定义工作流程），请点击（**切换工作流程**）**([switch workflow])**。
- “时间范围”(Time Range) - 要调整时间范围（如果未显示事件，则非常有用），请参阅更改时间窗口。
- 主机配置文件 - 要查看 IP 地址的主机配置文件，请点击 **主机配置文件**()，或者对于具有活动危害表现 (IOC) 标记的主机，点击该 IP 地址旁边显示的 **受损主机** 。
- “用户配置文件”（仅事件）- 要查看用户身份信息，请单击显示在**用户身份 (User Identity)** 旁的用户图标，或对于与 IOC 相关联的用户，请单击**红色用户 (Red User)**。
- 限制 - 要限制显示的列，请在要隐藏的列标题中点击 **关闭**（×） 在显示的弹出窗口中，点击 **Apply**。

  提示 要隐藏或显示其他列，请先选择或清除相应的复选框，然后点击**应用 (Apply)**。要将已禁用列添加回视图中，请展开搜索限制条件，然后点击“已禁用列”(Disabled Columns) 下的列名称。

- 向下展开 - 请参阅使用向下钻取页面。
- “排序”(Sort) - 要对工作流程中的数据排序，请点击列标题。再次点击列标题以反转排列顺序。
- “导航此页面”(Navigate This Page) - 请参阅工作流程页面遍历工具。
- “在页面之间导航”(Navigate Between Pages) - 要在当前工作流程中的页面之间导航，保留当前限制，请点击工作流程页面左上角相应的页面链接。
- “在事件视图之间导航”(Navigate Between Event Views) - 要导航至其他事件视图以查看关联事件，请点击**跳转至 (Jump to)** 并从下拉列表中选择事件视图。
- “删除事件”(Delete Events)（仅事件）- 要删除当前限制视图中的部分或全部项目，请选中要删除的项目旁边的复选框，然后点击**删除 (Delete)** 或点击**全部删除 (Delete All)**。

相关主题

工作流程页面
配置事件视图设置

查看 允许 列表事件

完成初始评估后，每当受监控的主机违反有效的 allow 名单，系统会生成 an *allow* 名单事件 。 名单事件是特殊类型的关联事件，会被记录到 管理中心 关联事件数据库中。

您可以使用 Cisco Secure Firewall Management Center查看合规 allow 名单事件表。然后，可根据要查找的信息操纵事件视图。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

访问 allow 名单事件时系统显示的页面取决于您使用的工作流程。可以使用预定义的工作流程，最终会产生事件的表视图。还可创建自定义工作流程，仅显示匹配特定需求的信息。

开始之前

您必须是 管理员、 安全分析师或 发现管理员 用户才能执行此任务。

过程

步骤 1 选择**分析** > **关联** > **允许列表事件**。

步骤 2 您有以下选择：

- 要执行基本工作流程操作，请参阅使用合规 允许 名单工作流程 ， 第 4 页。
- 要了解有关表中各列内容的详细信息，请参阅允许 名单事件字段 ， 第 6 页。
- 要查看更多选项，请右键单击表中的值。

允许 名单事件字段

允许 名单事件（您可以通过工作流程查看和搜索白名单事件）包含以下字段。

设备

检测到 allow 名单违规行为的受管设备的名称。

说明

说明 allow 名单是如何被违反的。例如：

```
Client “AOL Instant Messenger” is not allowed.
```

涉及应用协议的违规指明应用协议的名称和版本，以及所使用的端口和协议（TCP 或 UDP）。如果限制禁止某个特定的操作系统，描述中会包含操作系统的名称。例如：

```
Server "ssh / 22 TCP (OpenSSH 3.6.1p2)" is not allowed on Operating System
“Linux Linux 2.4 or 2.6”.
```

域

已变为不符合 allow 名单的主机的域。 仅当曾经配置 Cisco Secure Firewall Management Center以实现多租户时，此字段才存在。

主机重要性

用户向不符合 allow 名单的源主机所分配的主机重要性：“无”、“低”、“中” 或“高”。

IP 地址

已变为不符合 allow 名单的主机的 IP 地址。

策略

被违反的关联策略的名称，即包含该 allow 名单的关联策略。

端口

与触发应用协议 allow 名单违规（违规应用协议造成的违规）的发现事件关联的端口（如有）。对于其他类型的 allow 名单违规活动，该字段为空白。

优先级

策略或触发策略违规的 allow 名单所指定的优先级。根据关联策略中 allow 名单的优先级或关联策略自身的优先级来确定。请注意， allow 名单的优先级优先于策略的优先级。搜索此字段时，请输入 `none` 表示无优先级。

时间

allow 名单事件生成时的日期和时间。此字段不可搜索。

用户

登录已变为不符合 allow 名单的主机的任何已知用户的身份。

允许 名单

allow 名单的名称。

计数

与每行中所显示的信息匹配的事件数。请注意，“计数”(Count) 字段仅在应用了创建两个或多个相同行的约束后才显示。此字段不可搜索。

查看 允许 列表违规事件

系统会记录您的网络上的当前 *allow* 名单违规事件 。每个违规事件代表一个禁止在您的其中一台主机上运行的事件。如果主机变为合规，则系统将从数据库移除现已纠正的违规。

您可以使用 Cisco Secure Firewall Management Center 查看所有活动 allow 名单的 allow 名单违规事件表。然后，可根据要查找的信息操纵事件视图。

访问 allow 名单违规事件时显示的页面因使用的工作流程而异。预定义工作流程会产生主机视图，该视图包含符合限制条件的每台主机的配置文件。还可创建自定义工作流程，仅显示匹配特定需求的信息。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**分析** > **关联** > **允许列表违规**。

步骤 2 您有以下选择：

- 要执行基本工作流程操作，请参阅使用合规 允许 名单工作流程，第 4 页。
- 要了解有关表中各列内容的详细信息，请参阅允许 列表违规事件字段，第 8 页。
- 要查看更多选项，请右键单击表中的值。

允许 列表违规事件字段

可使用工作流程查看和搜索的允许 名单违规事件包含以下字段。

域

违规主机所在的域。 仅当曾经配置 Cisco Secure Firewall Management Center以实现多租户时，此字段才存在。

信息

与该 allow 名单违规事件相关的任何可用的供应商、产品或版本信息。对于违反 an allow 名单的协议，此字段还指出违规是由网络协议还是传输协议造成的。

IP 地址

违规主机的 IP 地址。

端口

与触发应用协议 allow 名单违规（违规应用协议造成的违规）的事件关联的端口（如有）。对于其他类型的 allow 名单违规活动，该字段为空白。

协议

与触发应用协 allow 名单违规（违规应用协议造成的违规）的事件关联的协议（如有）。对于其他类型的 allow 名单违规活动，该字段为空白。

时间

该 allow 名单违规事件被检测到的日期和时间。

类型

allow 名单违规事件的类型，即该违规事件是否由于下列内容不合规而导致：

- 操作系统 (os)（搜索此字段时，请输入 **os** 或 **operating system**。）
- 应用协议（服务器）
- 客户端
- 协议
- Web 应用 (web)（搜索此字段时，请输入 **web application**。）

允许 名单

被违反的 allow 名单的名称。

计数

与每行中所显示的信息匹配的事件数。请注意，“计数”(Count) 字段仅在应用了创建两个或多个相同行的约束后才显示。此字段不可搜索。

补救状态事件

当补救触发时，系统会将补救状态事件记录到数据库。可在“补救状态”(Remediation Status) 页面中查看这些事件。可搜索、查看和删除补救状态事件。

相关主题

补救状态表字段，第 10 页

查看补救状态事件

您在访问补救状态时看到的页面因使用的工作流程而异。可使用预定义的工作流程，其中包括补救的表视图。在表视图中，每个补救状态事件占一行。还可创建自定义工作流程，仅显示匹配特定需求的信息。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

开始之前

您必须是 管理员 用户才能执行此任务。

过程

步骤 1 选择**分析** > **关联** > **状态**。

步骤 2 或者，调整时间范围，如更改时间窗口中所述。

步骤 3 或者，要使用不同的工作流程，包括自定义工作流程，请按工作流程标题点击（**切换工作流程**）**([switch workflow])**。

提示 如果使用的是不包含补救表视图的自定义工作流程，则按工作流程标题点击（**切换工作流程**）**([switch workflow])** 菜单，然后选择**补救状态 (Remediation Status)**。

步骤 4 您有以下选择：

- 要了解有关显示的列的详细信息，请参阅补救状态表字段，第 10 页。
- 要对事件进行排序和限制，请参阅使用工作流程。
- 要导航至关联事件视图查看相关事件，请点击**关联事件 (Correlation Events)**。
- 要为当前页面添加书签以便快速返回该页面，请点击**将此页面加入书签 (Bookmark This Page)**。要导航至书签管理页面，请点击**查看书签 (View Bookmarks)**。
- 要根据表视图中的数据生成报告，请点击**报告设计器**，如从事件视图创建报告模板中所述。
- 要向下展开到工作流程中的下一个页面，请参阅使用向下钻取页面。
- 要从系统删除补救状态事件，请选中要删除的事件旁边的复选框，然后点击**删除 (Delete)** 或点击**全部删除 (Delete All)**，并确认要删除当前限制视图中的所有事件。
- 要搜索补救状态事件，请点击**搜索 (Search)**。

相关主题

使用工作流程

补救状态表字段

下表介绍补救状态表中可以查看和搜索的字段。

表 2: 补救状态字段

字段	说明
域	其受监控流量触发了策略违规（反过来又触发了补救）的设备的域。 仅当曾经配置 Cisco Secure Firewall Management Center以实现多租户时，此字段才存在。

字段	说明
策略	已违反并触发补救的关联策略的名称。
补救名称	已发起的补救的名称。
结果消息	描述在发起补救后所发生情况的消息。状态消息包括： • 补救成功完成 • 提供给补救模块的输入出错 • 补救模块配置出错 • 登录远程设备或服务器时出错 • 无法在远程设备或服务器上获得所需权限 • 登录远程设备或服务器时超时 • 执行远程命令或服务器时超时 • 远程设备或服务器不可达 • 已尝试补救，但是失败 • 未能执行补救程序 • 未知/意外错误 如已安装自定义补救模块，则可能出现自定义模块实现的其他状态消息。
规则	触发了补救的关联规则的名称。
时间	Cisco Secure Firewall Management Center发起补救的日期和时间。
计数	与每行中所显示的信息匹配的事件数。请注意，“计数”(Count) 字段仅在应用了创建两个或多个相同行的约束后才显示。此字段不可搜索。

相关主题

事件搜索

使用补救状态事件表

您可以更改事件视图的布局或按字段值限制视图中的事件。

当禁用列时，除非稍后重新添加该列，否则该列在会话持续时间内处于禁用状态。如果禁用第一列，则会添加“计数”(Count) 列。

请注意，在表视图中点击某一行中的一个值时，会限制该表视图，且不会向下展开到下一个页面。

提示 表视图的页面名称中始终包含“Table View”。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

开始之前

您必须是 管理员 用户才能执行此任务。

过程

步骤 1 选择**分析** > **关联** > **状态**。

提示 如果使用的是不包含补救表视图的自定义工作流程，则按工作流程标题点击（**切换工作流程**）**([switch workflow])** 菜单，然后选择**补救状态 (Remediation Status)**。

步骤 2 您有以下选择：

- 要了解有关显示的列的详细信息，请参阅补救状态表字段，第 10 页。
- 要对事件进行排序和限制，请参阅使用工作流程。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。